



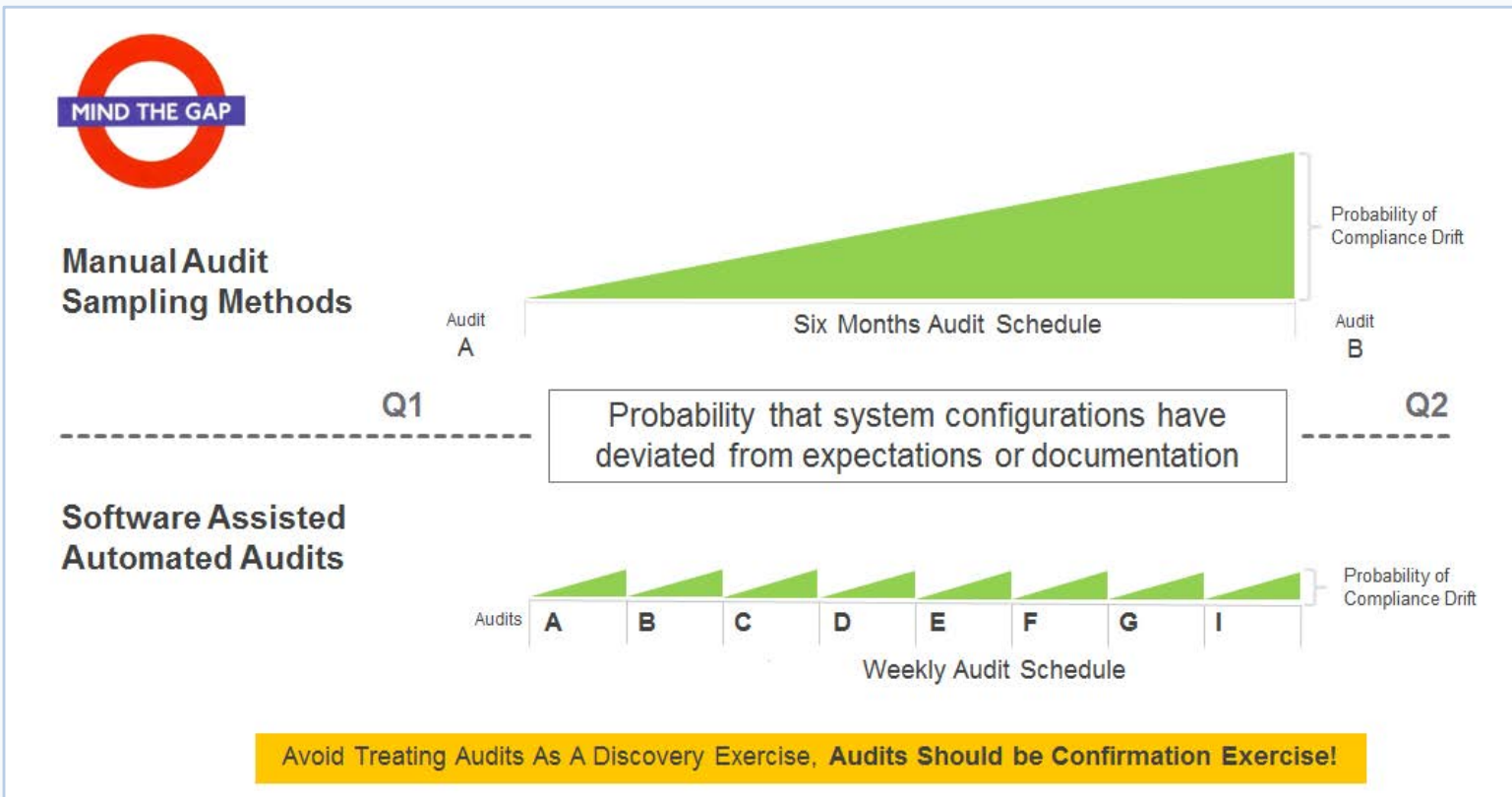
QUALYS SECURITY CONFERENCE 2020

Continuous Compliance in Hybrid Environment

Shailesh Athalye

VP, Compliance Solutions, Qualys, Inc

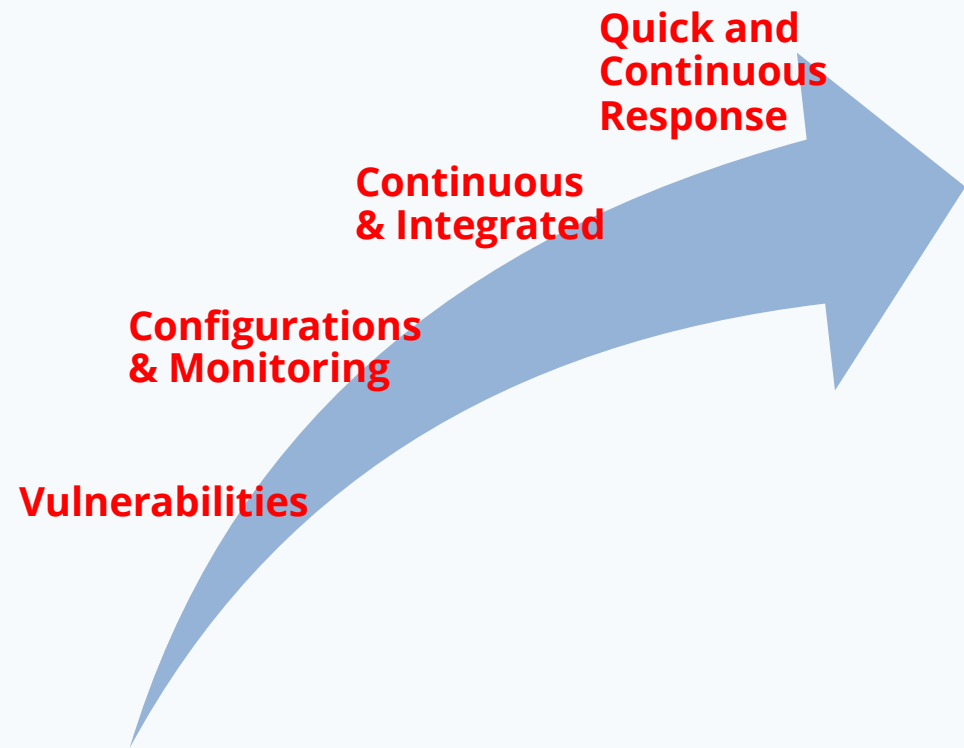
2014: Good Old Days of Compliance



2020: Matured Cybersecurity Risk Management

Performing vulnerability management with a context to reduce the “attack surface”

Quick continuous assessment and fix cycles before images are in production



Teams Speak Different Languages



Elastic, Kafka, custom
web servers



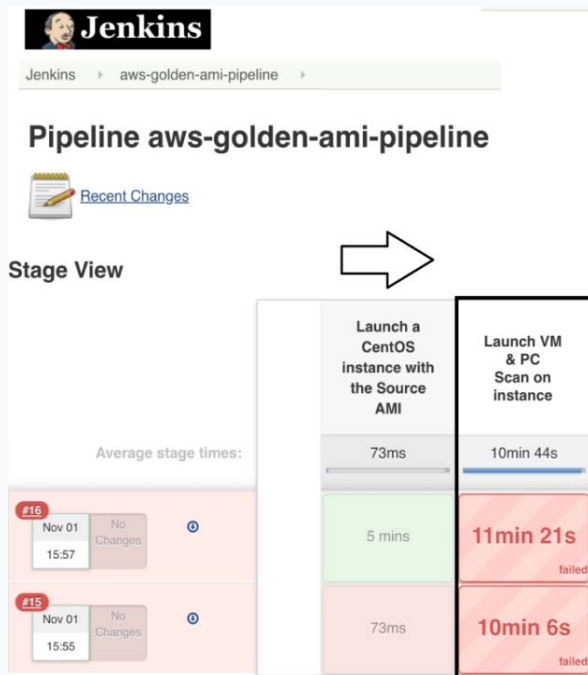
Identify risk and
compliance



Secure hosts, config/integrity/
vulnerability management

Security & Compliance assessment should be baked into DevOps

Start Compliant, Stay Compliant

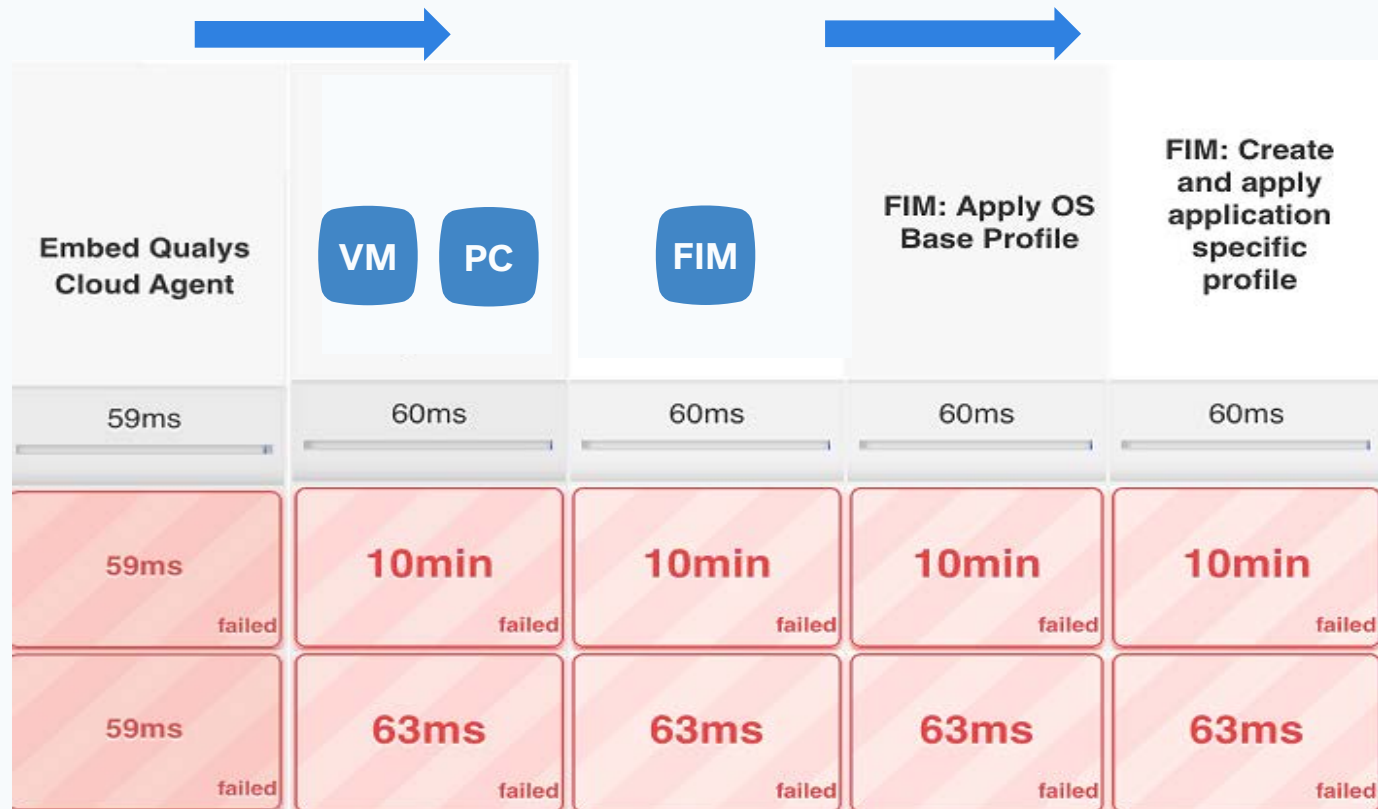


QUALYS POLICY COMPLIANCE RESULTS

Show 10 entries

CID	Title	Technology	Criticality
14602	Status of the 'nosuid' option for '/tmp' partition using 'mount' command	CentOS 7	4
10804	Status of the SELinux current mode (running configuration)	CentOS 7	4
10643	Status of iptables package	CentOS 7	4
12815	List of runtime audit rules for '/etc/passwd' file, using auditctl	CentOS 7	4
10664	Status of the 'OPTIONS' setting within '/etc/sysconfig/chronyd' file	CentOS 7	4
9473	Existence of the 'extraneous' files and directories (Sensitive files/Directories)	Tomcat 8	3
9477	Status of 'X-Powered-By' setting within 'server.xml' file	Tomcat 8	4
9551	Status of the 'secure' attribute for each 'Connector' elements whose 'SSL Enabled' are set to 'true'	Tomcat 8	4
9605	Status of the command-line flag 'STRICT_SERVLET_COMPLIANCE' set for the Tomcat process	CentOS 7	4
9565	Status of the 'web server processes' which are not started with 'Security Manager'	CentOS 7	4

Monitor Critical Files From CD Phase



Security Control Validation (SCV)

Top five responsibilities of CISOs

<https://www.bitsight.com/blog/ciso-roles-and-responsibilities>

Pre-requisites and configurations

Native security features

The screenshot displays the 'Policy Compliance' interface, specifically the 'Reports' section. A sidebar on the left shows a summary of 23 total control instances, categorized by 'Anti-Virus/Malwa...', 'CRITICALITY' (Serious: 2, Critical: 19, Urgent: 2), and 'POSTURE' (Pass: 11, Fail: 12). The main area, titled 'Control View', shows a search filter for 'pc.control.category: "Anti-Virus/Malware"'. Below this is a table of control instances with columns for Status, CID, Control, Technology/Instance, Asset Name, and Last Evaluation. The table lists several failed controls related to Internet Explorer settings and system ASLR settings on Windows Server 2012 R2, and some passed controls related to antivirus settings and security patches on Mac OS X 10.x.

STATUS	CID	CONTROL	TECHNOLOGY/INSTANCE	ASSET NAME	LAST EVALUATION
FAIL	9043	Status of the 'Default Protections for Internet Explorer' setting.	Windows Server 2012 R2 os	i-6f91d2a8 10.11.114.112 i-6f91d	Apr 16, 2019
FAIL	9043	Status of the 'Default Protections for Internet Explorer' setting.	Windows Server 2012 R2 os	win2012r2 10.10.35.201 WIN2012	Oct 07, 2017
FAIL	9057	Status of the 'System ASLR' setting.	Windows Server 2012 R2 os	i-6f91d2a8 10.11.114.112 i-6f91d	Apr 16, 2019
FAIL	9057	Status of the 'System ASLR' setting.	Windows Server 2012 R2 os	win2012r2 10.10.35.201 WIN2012	Oct 07, 2017
FAIL	4156	Status of the 'Notify antivirus programs when opening attachments' Group Policy setting.	Windows Server 2012 R2 os	i-6f91d2a8 10.11.114.112 i-6f91d	Apr 16, 2019
FAIL	4156	Status of the 'Notify antivirus programs when opening attachments' Group Policy setting.	Windows Server 2012 R2 os	win2012r2 10.10.35.201 WIN2012	Oct 07, 2017
PASS	8881	Status of the security patches and software updates.	Mac OS X 10.x os	10.10.10.37	Jul 24, 2017
PASS	8844	Status of the 'Automatically check for updates' setting.	Mac OS X 10.x os	10.10.10.37	Jul 24, 2017
FAIL	8860	Status of the Gatekeeper feature.	Mac OS X 10.x os	10.10.10.37	Jul 24, 2017
FAIL	8861	Status of the safe download list's (XProtect) last	Mac OS X 10.x	10.10.10.37	Jul 24, 2017

Anti-virus | FIM Agents | Splunk | Kafka | Native Malware Protection | Jenkins

STEP 4 / 5

- 1 Basic Information
- 2 Select Assets
- 3 Select Controls
- 4 Schedule
- 5 Review and Confirm

Schedule

Schedule the remediation job to run on demand or in the future

On Demand

Schedule

Remediation Window

You can configure a remediation window to run to

☒ None ☐ Set Duration

Note: Not setting the patch window will allow the cloud agent to take as much time as it needs to complete the job.

Cancel

Previous

Next

The background is a solid blue color with a repeating pattern of small white dots. The dots are arranged in a grid-like fashion, with some dots slightly offset to create a sense of depth or movement.

New Policy Compliance UI

Security for Inaccessible & Exotic Hosts

Use APIs/UI and push data to Qualys

- Create custom assets
- Push command output, vulnerability, config data

Qualys Out-of-Band Config Assessment (OCA)

The screenshot displays the HP Qualys OCA interface. At the top, the HP logo is visible. Below it, the 'Detailed Results' section shows the IP address 154.36.214.3 (hp-in01-prn02, HP-IN01-PRN02) and the device name HP FutureSmart 4. A summary bar indicates a 'PASS' status with 12 passed controls, 2 failed, and 0 errors. The interface lists tracking details: Tracking Method: OCA, Last Scan Date: 09/05/2019 at 11:12:12 (GMT+0530), Qualys Host ID: c9192ca4-8bf4-454c-82fa-8c31003521fa, and Asset Tags: OCA. A table of controls is shown below, with a total of 12 controls, 12 passed (100%), 0 failed, 0 errors, 0 approved exceptions, and 0 pending exceptions. The '1. System Configuration' section is expanded, showing a list of controls with their status and severity.

Control ID	Description	Severity	Status
(1.1) 1116	Status of the 'File Transfer Protocol (FTP)' service	CRITICAL	PASS
(1.2) 1861	Status of the 'telnet' service	CRITICAL	FAIL
(1.3) 10270	Status of the SNMP community strings	SERIOUS	PASS
(1.4) 12413	Status of the 'AppleTalk' protocol	SERIOUS	PASS
(1.5) 13857	Status of version of firmware stored in boot PROM	CRITICAL	PASS
(1.6) 14039	Status of SNMP configuration of version SNMPv1	CRITICAL	PASS

Validate settings and data

Report vulnerabilities, security and misconfigurations

New-Age File Integrity Monitoring

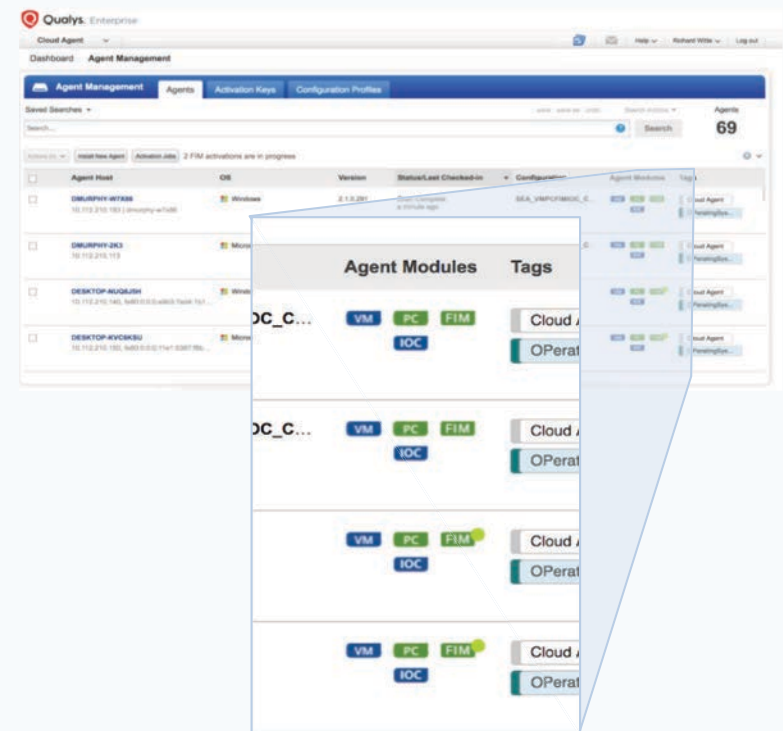
Built on the same Qualys Cloud Agent you use for VM, PC, Inventory

Real-time detection for high volume, high scale

Automated incident management and alerting

Out of the box PCI monitoring profiles for OS and applications

No infrastructure or data load for you to manage



Authorized vs Unauthorized Changes

Qualys. Express

File Integrity Monitoring ▾

DASHBOARD EVENTS RULES INCIDENTS REPORTS ASSETS CONFIGURATION

Incidents

101
Total Incidents

STATUS
CLOSED 100
OPEN 1

All Incidents Correlation Rules

ruleId:8fc42fcc-4028-45e8-88da-672254ed1493

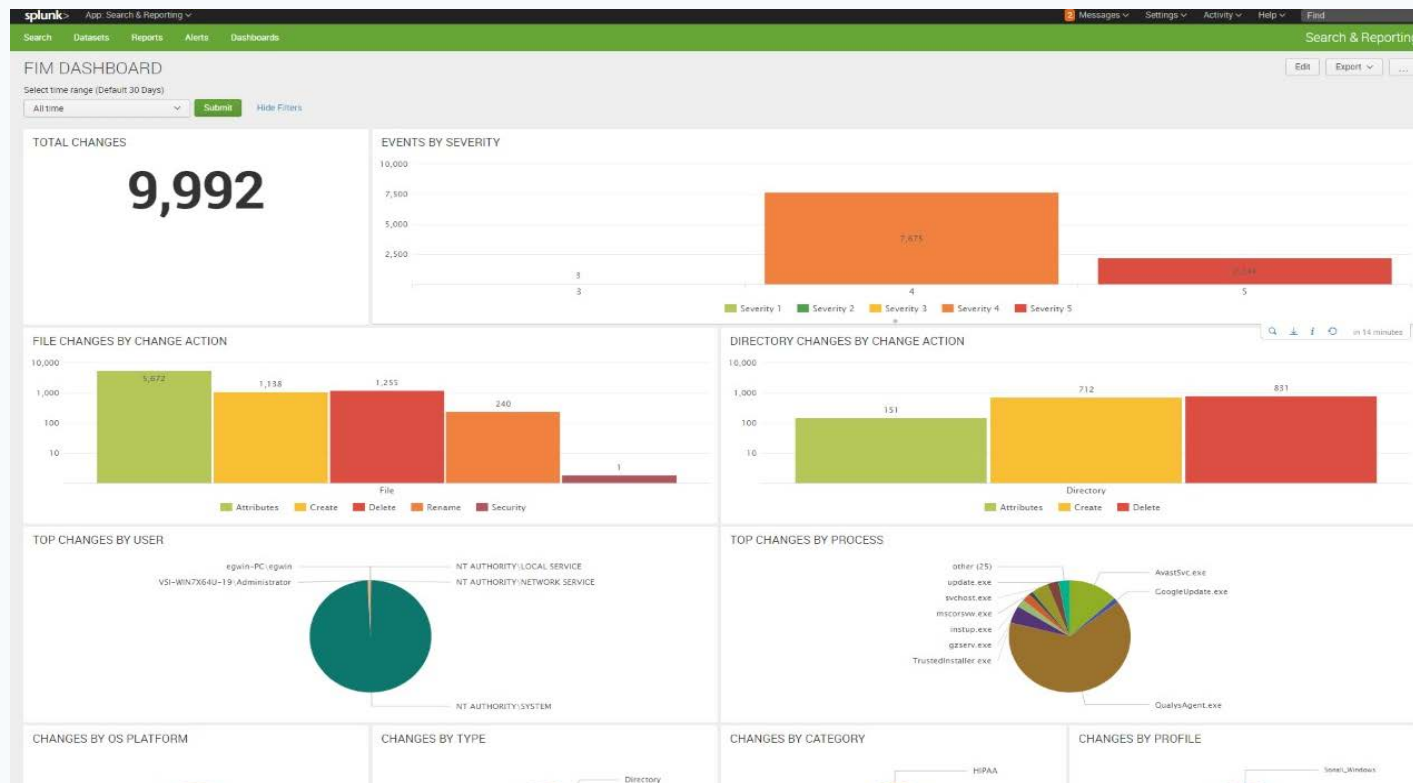
Assigned to me
101

Pending
1

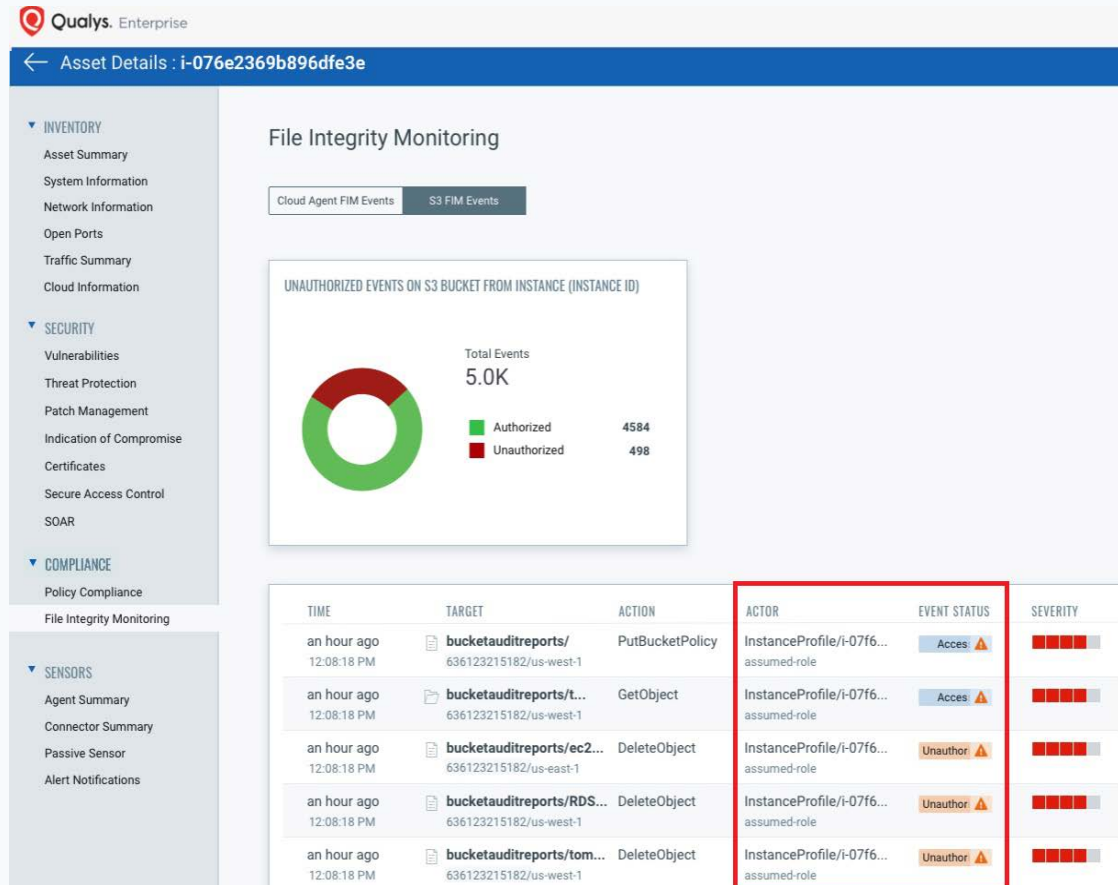
1 - 50 of 101

CREATED	NAME	TYPE	STATUS	ASSIGNEE	DISPOSITION	CHANGE TYPE	APPROVAL
21 hours ago 10:30:00 AM	Unauthorized Windows Patc...	AUTOMATED	OPEN	quays_qd		-	-
2 days ago 10:30:00 AM	Unauthorized Windows Patc...	AUTOMATED	CLOSED	quays_qd	PATCHING	AUTOMATED	POLICY_VIOLA...
3 days ago 10:30:00 AM	Unauthorized Windows Patc...	AUTOMATED	CLOSED	quays_qd	PATCHING	AUTOMATED	POLICY_VIOLA...
4 days ago 10:30:00 AM	Unauthorized Windows Patc...	AUTOMATED	CLOSED	quays_qd	PATCHING	AUTOMATED	POLICY_VIOLA...
5 days ago 10:30:00 AM	Unauthorized Windows Patc...	AUTOMATED	CLOSED	quays_qd	PATCHING	AUTOMATED	POLICY_VIOLA...
6 days ago 10:30:00 AM	Unauthorized Windows Patc...	AUTOMATED	CLOSED	quays_qd	PATCHING	AUTOMATED	POLICY_VIOLA...
7 days ago 10:30:00 AM	Unauthorized Windows Patc...	AUTOMATED	CLOSED	quays_qd	PATCHING	AUTOMATED	POLICY_VIOLA...

Open APIs for Integration



Context of Changes in Cloud

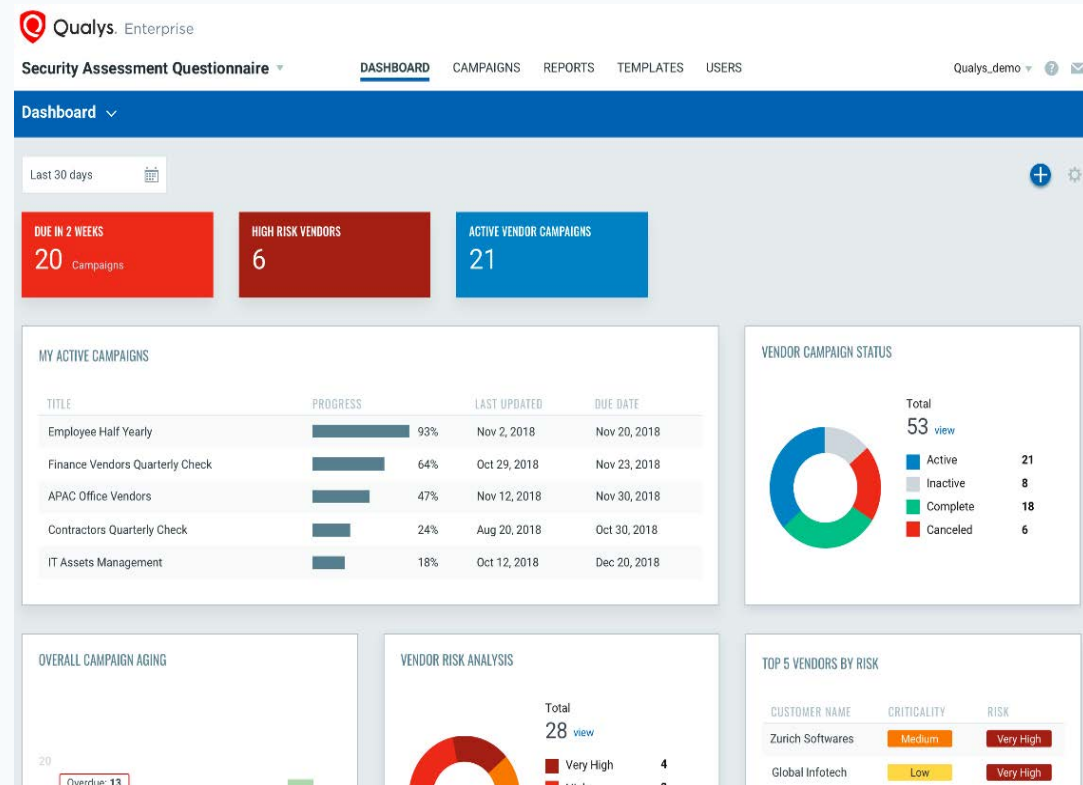


Assess Vendor Security

Manage vendor risk per
vendor criticality

Unify Vendor security and
process compliance with
technical security

Qualys Security Assessment Questionnaire (SAQ)



SaaS Applications Challenges

Public cloud spending skyrockets as SaaS shines



IDC: Cloud spending to grow 21% by 2021



Office 365

box



Microsoft, Google Make Cloud Offerings More Enticing



HR gets the cloud treatment

THE AUSTRALIAN

Workday Rises on Demand for Business Cloud-Based Software

Bloomberg



Spending On CRM Apps Predicted To Soar In 2018

COMPUTERWORLD



SaaS Security and Compliance

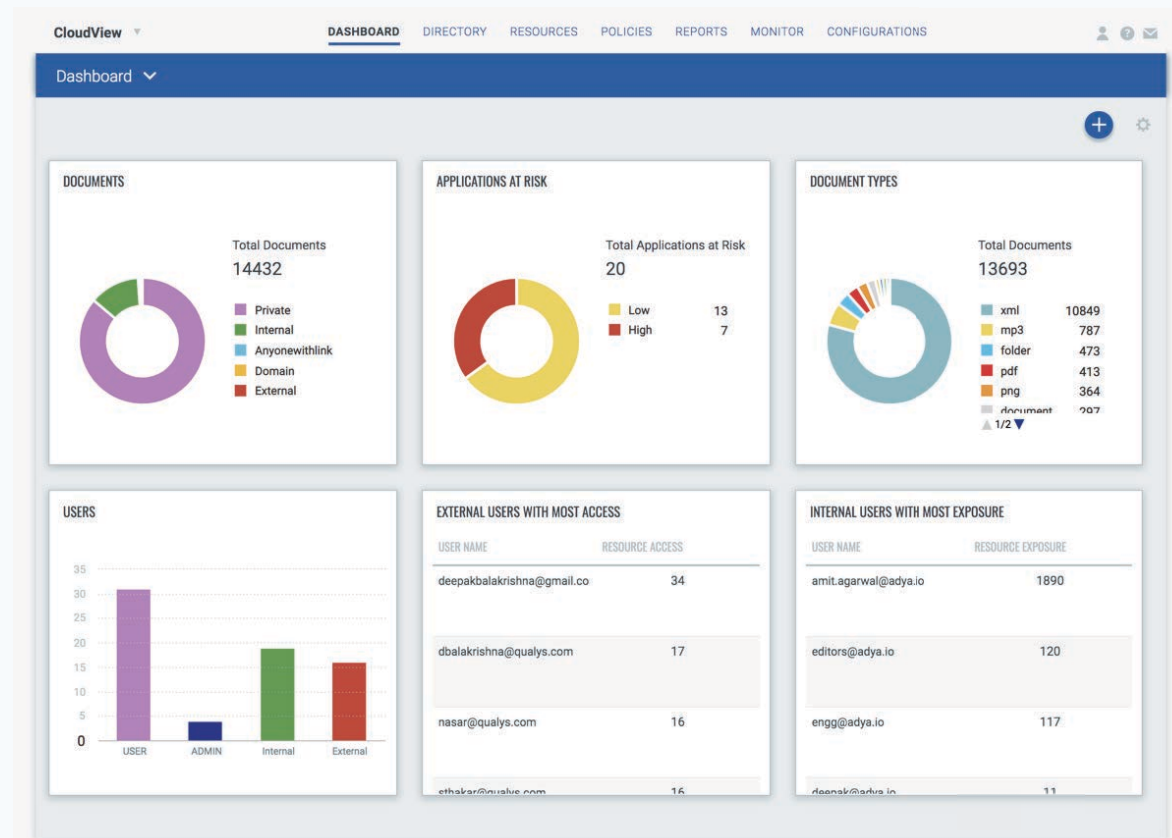
Inventory

Access

Exposure

Security Configurations

Office365, Google Suite, Salesforce
GitHub, Okta, Slack



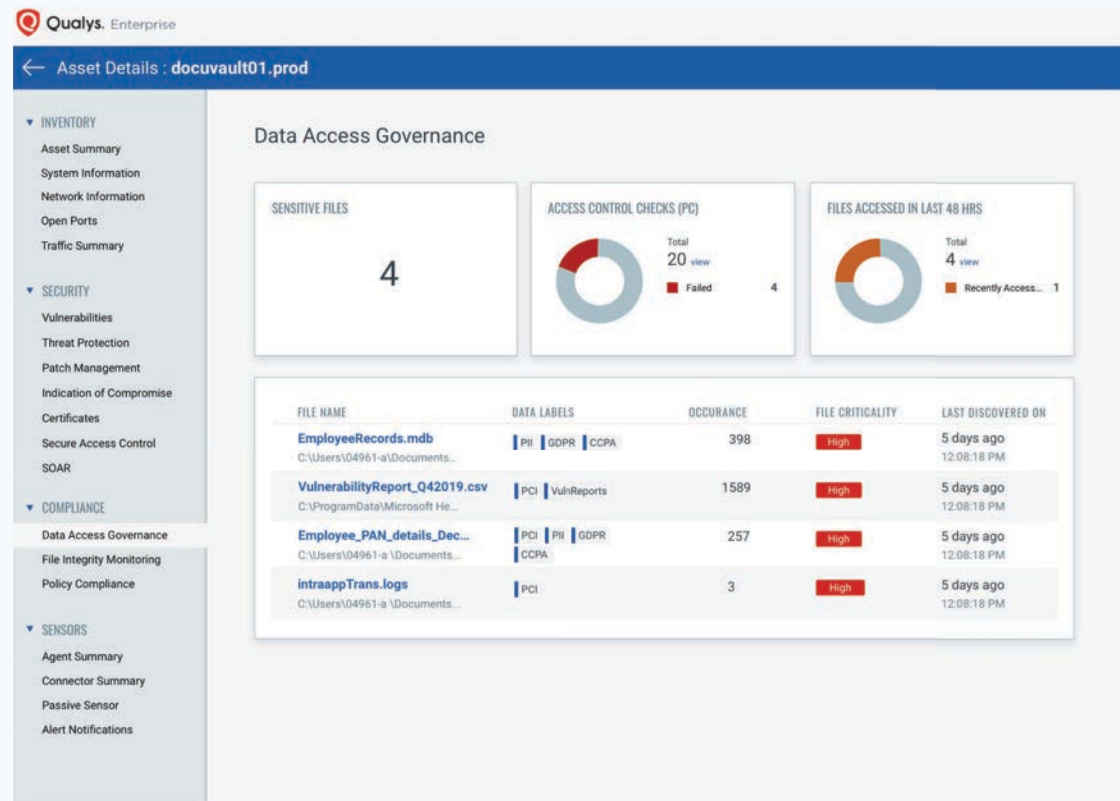
Sensitive Data Discovery and Security

Discovery

Access Visibility

Activity Monitoring

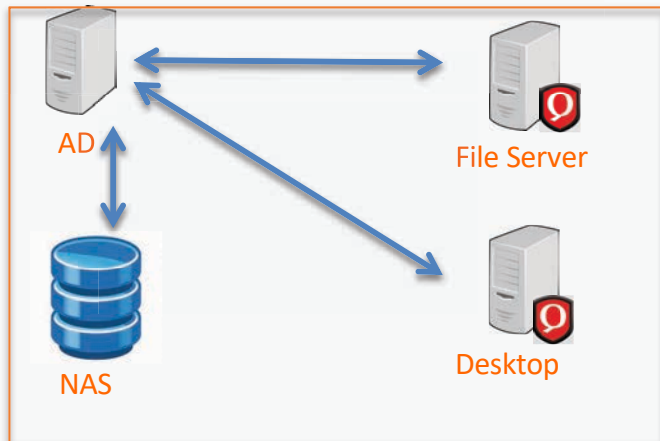
Context for security



Cloud Applications



Qualys Agent (MFT)



On Premises Unstructured Data

Directory / Metadata / Access / Classification
Adya/CV/CloudTrail

Directory / Metadata / Access / Based on rules

Qualys Cloud Platform

Unstructured Data Discovery

Visibility in ITAM – know assets hold sensitive data

Secure through PC - Create permission/share/access controls to check their access

Compliance
GDPR / CCA / HIPAA/ etc

Monitor through FIM

Quick Demo



QUALYS SECURITY CONFERENCE 2020

Thank You

Compliance Team and Shailesh Athalye
sathalye@qualys.com